COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

JOHN NAIMO
ACTING AUDITOR-CONTROLLER

June 5, 2014

TO: Supervisor Don Knabe, Chairman
Supervisor Gloria Molina
Supervisor Mark Ridley-Thomas
Supervisor Zev Yaroslavsky
Supervisor Michael D. Antonovich

FROM: John Naimo
Acting Auditor-Controller

SUBJECT: **COUNTY'S ANNUAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PROGRAM REPORT FOR CALENDAR YEAR 2013**

This memo provides an update on the County's Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Program for the year ended December 31, 2013. As you are aware, the Chief HIPAA Privacy Officer (CHPO) and associated responsibilities reside with the Auditor-Controller (A-C). In this report, we apprise your Board of the implementation efforts to recent changes in regulations and responsibilities imposed to the County by those changes, annual breach reports provided to the U.S. Department of Health and Human Services (DHHS), a list of recent audits, and notification to your Board about important developments within the County's HIPAA Privacy Program.

Background

The County is fundamentally compliant with the Privacy Rule. However, due to the County's size and structure, the CHPO and the Chief Information Security Officer (CISO) within the Chief Information Office (CIO), who has oversight of the HIPAA Security Rule, face challenges related to the complexity of implementing significant changes in the regulations (see below). The challenges are due to program and regulation mandates including ongoing assessments, countywide limited resources, departmental cooperation, and employee training.

The County departments, divisions, and certain commissions that must comply with HIPAA are:

- A-C's divisions and personnel who perform business associate functions,
- Chief Executive Office
- CIO
- County Counsel
- Executive Office of the Board, Children's Special Investigation Unit
- Executive Office of the Board, HIV Commission
- Department of Health Services (DHS)
- Department of Human Resources' (DHR) Employees' Flexible Spending Accounts within the Employee Benefit's Division, a small health plan per HIPAA,
- Internal Services Department's (ISD) divisions and personnel who perform business associate functions
- Department of Mental Health (DMH)
- Probation Department's Dorothy Kirby Center
- Probation Department's Electronic Medical Record System
- Department of Public Health (DPH)
- Sheriff's Department's Pharmacy Division of the Medical Services Bureau
- Treasurer and Tax Collector's divisions and personnel who perform business associate functions.

Ongoing Implementation of the Omnibus Rule

On January 17, 2013, the Office for Civil Rights (OCR) of DHHS issued the Omnibus Final Rule (Rule) implementing changes in regulations under HIPAA pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The changes were extensive as they significantly strengthen privacy protections for patient health information while enhancing DHHS' ability to enforce such protections. The Rule was effective on March 26, 2013, with a compliance date for most provisions on September 23, 2013.

Omnibus Rule Implementation of Business Associate Functions and Agreements

When the HIPAA regulations were originally enacted, only covered entities were required to adhere to the law. That left many entities with ongoing access to protected health information (PHI), such as billing agencies, information technology companies, and labs outside the scope and jurisdiction of HIPAA. Although covered entities were required to enter into agreements with these business associates to whom they provided medical information, DHHS did not have jurisdiction to enforce or penalize business associates for non-compliance of the HIPAA regulations or the contract with the covered entity. To correct this issue, the Rule amended HIPAA so that business associates (including County departments performing business associate functions) are

now directly liable for most HIPAA requirements. Specifically, those provisions related to safeguarding PHI and breach notification.

The Rule also expanded the definition of business associate to include downstream subcontractors of business associates. It imposes direct liability on business associates and downstream vendors for violations of certain provisions, with maximum civil fines of up to $1.5 million per year.

If an agreement was not in place at that time or up for renewal, the Rule required covered entities to revise their business associate agreements to include the updated language. However, for agreements that were in place as of January 2013 and included the interim final rule language, the Rule gave covered entities up to September 2014 to amend those agreements. Nevertheless, the CHPO, CISO, and County Counsel determined that it was in the best interest of the County to have departments amend their contracts to include the Rule's revised language as soon as possible. To that end, the departments completed the task on or before September 23, 2013. The departments have until September 23, 2014 to amend the language. In addition, ISD's master agreement includes the updated HIPAA language.

Omnibus Rule Breach Notification Requirements

The Rule significantly modified the Breach Notification Rule to limit the discretion of covered entities to decide whether or not a breach must be reported. Prior to the Rule, covered entities were required to report each breach that was determined by the covered entity to have the potential of causing harm to the patient. The Rule omitted the subjective harm determination and now requires that **any** impermissible disclosure of PHI is presumed to be a reportable breach to DHHS and the patient.

The Rule requires the County to provide notice of breaches of unsecured PHI to DHHS on an annual basis or within 60 days of a breach impacting 500 or more individuals. The reports are due by March 1st to DHHS for those breaches that occurred in the previous calendar year. For the 2013 calendar year, a total of 11 breaches were reported to DHHS versus a total of four breaches reported for the 2012 calendar year. The increase is due to the changes in the regulations and reporting requirements.

HIPAA Training Program

According to the regulations, the County must train workforce members on the HIPAA and HITECH Act regulations and related policies and procedures to the extent necessary and appropriate for its employees to carry out their functions. The health care component departments, with the exception of DHS, utilize the County's Learning Management System (LMS) to train their workforce members. DHS offers LMS training to certain employees and a self-study guide to their workforce members who do not have regular access to a computer. Approximately 35,000 County workforce members

receive some form of HIPAA training on an annual basis. This includes providing training on updates or changes to the Privacy Rule regulations. Due to the changes in the HIPAA regulations noted above, the HIPAA departments were required to train their applicable and active workforce members on the Rule prior to September 23, 2013. The HIPAA departments reported an average of 94.5% of their workforce members completed training by the deadline. Many of the employees who did not complete training by the deadline were on extended leave, or were newly hired at the time of our survey, and must complete the training within 90 days of beginning County service. The CHPO continues to work closely with County departments to ensure that all covered workforce members complete the require training.

At this time, the LMS-HIPAA training does not include State or other privacy laws that may apply to departments. Thus, each department must develop training materials that informs their employees about privacy laws that they must adhere to. Further, departments must develop a method to ensure that employees are educated on County and departmental policies and procedures. The CHPO, County Counsel, and CISO provide assistance, guidance, and approve the departments' HIPAA training programs to the extent they include HIPAA and HITECH Act content.

HIPAA/HITECH Act Privacy and Security Committee

The CHPO and CISO jointly established a HIPAA/HITECH Act Privacy and Security Committee (Committee) consisting of representatives from each of the health care component departments. The Committee meets monthly to inform departments about the changes in regulations, implementation and standard requirements, privacy and security policies and procedures updates, enforcement, and upcoming privacy and security laws that may impact the County's and covered departments' HIPAA programs.

HIPAA Privacy Rule Audits Conducted in 2013

For the 2013 calendar year, the A-C HIPAA Compliance Unit (HCU) conducted Privacy Rule audits:

- DPH: Hollywood Wilshire Public Health Center
- DPH: Nurse-Family Partnership Program
- DPH: Torrance Public Health Center
- DMH: Compton Family Mental Health Center
- DMH: Enhanced Specialized Foster Care Program
- DMH: Edelman's Children's Mental Health Program
- DMH: Edelman's Adult Mental Health Program
- DHS: LAC+USC Medical Center

The HCU also conducts unannounced onsite facility reviews to ensure that County clinics and hospitals are posting their notices of privacy practices according to HIPAA

standards. For the 2013 calendar year, the CHPO visited 16 facilities. Of those facilities, ten did not post the notice pursuant to the HIPAA standards. If there is a finding that a facility or program is not in compliance with the regulations or standards, the CHPO will coordinate with the department's designated privacy and compliance officers in the development of a corrective action plan, and will follow-up until all issues are adequately resolved.

HIPAA Privacy Complaints and Investigations

CHPO is responsible for responding and investigating complaints and queries from OCR, clients, individuals, and County workforce members. Complaints received by this Office are made through the HIPAA Hotline, HIPAA e-mail address (hipaa@auditor.lacounty.gov), in-person filing, or by mail. Covered departments also maintain a log of complaints that are reported to the CHPO should the incident be reportable to the DHHS.

For the 2013 calendar year, the CHPO's office received and logged 55 complaints. This is a significant increase from the prior year, where we received 33 complaints. All complaints and issues were resolved and/or reported accordingly. The most common patient complaint against the County involved allegations that employees either improperly disclosed the patient's PHI to unauthorized persons or employees accessed medical records without a legitimate reason. The most common employee self-reporting incidents involved the loss/theft of computer devices, or loss of paper files that contained confidential information.

Enforcement and Penalties for Non-compliance

DHHS enforces HIPAA and the HITECH Act and may issue fines and penalties with maximum civil fines of up to $1.5 million per year. DHHS considers a number of factors in deciding whether to issue fines and penalties for a breach, including the adequacy of the covered entity's compliance infrastructure. To date, no penalties or fines have been issued against the County for non-compliance.

Next Steps

The CHPO and CISO drafted proposed County HIPAA policies to ensure that covered departments and staff are aware of and comply with the Rule's requirements. The policies were cleared with the CEO's Employee Relations Division, who distributed them to the impacted unions. They also were vetted through the HIPAA Privacy and Security Committee, which is comprised of representatives from the HIPAA departments. Finally, County Counsel approved the policies. The draft policies include requirements for employee training, safeguarding PHI, and discipline of workforce members who do not comply with the Privacy and Security Rules. We will present the draft policies to the

Health Deputies, Public Safety Deputies, Children and Families' Well-Being Deputies, and the Audit Committee prior to sending them to your Board for final approval.

Notable Events Since December 31, 2013

As your Board is aware, on February 25, 2014, a County business associate, Sutherland Healthcare Solutions provided confirmation to the CHPO of a breach that included County patient information. At this time, the total number of County patients impacted by the breach is approximately 342,000. Individual notices were mailed to the patients whose addresses were available. For those patients whose addresses were not found, DHS and DPH provided notice of the breach on their websites. The media was notified through three separate press releases. The CHPO notified DHHS according to the HIPAA breach notification requirements. Due to pending litigation and the ongoing criminal investigation by the District Attorney's Cyber Investigation Response Team and the Torrance Police Department, this matter is under the direction of County Counsel. To the extent that this matter pertains to the HIPAA Privacy Rule, we will also provide your Board with supplemental information in our next annual report.

Further, the recent Board motion entitled *Protecting Sensitive Personal and Public Health Information* impacts the HIPAA program as it pertains to the safeguarding of PHI. The CHPO will work with the CISO to the extent requested and needed to fulfill the requirements of the motion.

Summary and Conclusion

Open communication between the CHPO and the covered departments is critical in ensuring compliance with the regulations and the success of the County's HIPAA Program. In addition, it is essential for departments to provide up-to-date and regular training to workforce members on the standards, policies, and procedures to safeguard PHI. We encourage the departments to timely and routinely notify the CHPO about privacy complaints and privacy breaches. Further, we remind departments to document complaints and their resolutions and perform self-audits to ensure compliance with the regulations.

The County's HIPAA/HITECH Act Program continues to advance awareness of health privacy matters through the Committee, training, and the audit programs. The CHPO is responsive to departments, individuals, workforce members, privacy and security taskforces, DHHS, and your Board in resolving privacy complaints and concerns. The CHPO will continue to work with the CISO and County Counsel to implement the HITECH Act regulations to the departments and appropriately address areas of weakness as they are discovered through audits, employee vigilance, and client complaints.

Please call me if you have questions, or your staff may contact Linda McBride, CHPO, at (213) 974-2166.

JN:RC:GZ:LTM

c: William T Fujioka, Chief Executive Officer
John L. Scott, Sheriff
John Krattli, County Counsel
Mitchell H. Katz, M.D., Director, Department of Health Services
Jonathan E. Fielding, M.D., Director, Department of Public Health
Sachi A. Hamai, Executive Officer, Executive Office of the Board
Jerry Powers, Chief Probation Officer
Dr. Marvin J. Southard, Director, Department of Mental Health
Lisa M. Garrett, Director of Personnel, Department of Human Resources
Richard Sanchez, Chief Information Officer
Jim Jones, Director, Internal Services Department
Mark Saladino, Treasurer and Tax Collector